Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

A Survey on Reducing Routing Distraction in IP Networks using Cross-Layer Methodology

Mr. Sagar M. Bhakre[1], Asst. Prof. C. Sarathkumar[2]
[1]Computer Science and Engineering, SKEC, Khammam
[2]Computer Science and Engineering, SKEC, Khammam

Abstract— Backup paths are widely used in IP networks to protect IP links from failures. However, existing solutions such as the commonly used independent model and Shared Risk Link Group (SRLG) model do not accurately reflect the correlation between IP link failures, and thus may not choose reliable backup paths. A cross-layer approach is proposed for minimizing routing disruption caused by IP link failures. A probabilistically correlated failure (PCF) model is developed to quantify the impact of IP link failure on the reliability of backup paths. With the PCF model, an algorithm is proposed to choose multiple reliable backup paths to protect each IP link. When an IP link fails, its traffic is split onto multiple backup paths to ensure that the rerouted traffic load on each IP link does not exceed the usable bandwidth. This approach using real ISP networks with both optical and IP layer topologies. Experimental results show that two backup paths are adequate for protecting a logical link. Compared with existing works, the backup paths selected by approach are at least 18 percent more reliable and the routing disruption is reduced by at least 22 percent.

Keywords— Routing, failures, cross-layer, recovery, IP networks

I. INTRODUCTION

IP link failures are fairly common in the Internet for various reasons. In high speed IP networks like the Internet backbone, disconnection of a link for several seconds can lead to millions of packets being dropped. Therefore, quickly recovering from IP link failures is important for enhancing Internet reliability and availability, and has received much attention in recent years. Currently, backup path-based protection and is widely used by Internet Service Providers (ISPs) to protect their domains. In this approach, backup paths are pre-computed, configured, and stored in routers. When a link failure is detected, traffic originally traversing the link is immediately switched to the backup path of this link. Through this, the routing disruption duration is reduced to the failure detection time which is typically less than 50 ms. Selecting backup paths is a critical problem in backup path-based protection.

Selecting backup paths is a critical problem in backup path-based protection. Existing approaches mainly focus on choosing reliable backup paths to reduce the routing disruption caused by IP link failures. However, they suffer from two limitations. First, the widely used failure models do not accurately reflect the correlation between IP link failures. As a result, the selected backup paths may be unreliable. Second, most prior works consider backup path selection as a connectivity problem, but ignore the traffic load and bandwidth constraint of IP links.

Current IP backbone networks are primarily built on the Wavelength Division Multiplexing (WDM) infrastructure. In this layered structure, the IP layer topology (logical topology) is embedded on the optical layer topology (physical topology), and each IP link (logical link) is mapped to a light path in the physical topology. An IP link may consist of multiple fiber links, and a fiber link may be shared by multiple IP links. When a fiber link fails, all the logical links embedded on it fail simultaneously. An example of the topology mapping in IP-over-WDM networks. The logical topology is embedded on the physical topology in which nodes v5, v6, andv7 are optical layer devices and hence do not appear in the logical topology. Logical links are mapped to light paths.

II. RELATED WORK

A) A CROSS-LAYER APPROACH FOR IP NETWORK PROTECTION

Backup paths are widely used to protect IP links from failures. Existing solutions such as the commonly used independent and Shared Risk Link Group models do not accurately reflect the correlation between IP link failures, and thus may not choose reliable backup paths. We propose a cross-layer approach for IP link protection. We develop a correlated failure probability (CFP) model to quantify the impact of an IP link failure on the reliability of backup paths. With the CFP model, we propose two algorithms for selecting backup paths. The first algorithm focuses on choosing the backup paths with minimum failure probability. The second algorithm further considers the bandwidth constraint and aims at minimizing the traffic disruption caused by failures. It also ensures that the rerouted traffic load on each IP link does not exceed the usable bandwidth to avoid interfering with the normal traffic. Simulations based on real ISP networks show that our approach can choose backup paths that are more reliable and achieve better protection.

B) MINIMIZING PROBING COST AND ACHIEVING IDENTIFIABILITY IN PROBE BASED NETWORK LINK MONITORING

Continuously monitoring the link performance is important to network diagnosis. Recently, active probes sent between end systems are widely used to monitor the link performance. In this paper, we address the problem of minimizing the probing cost and achieving identifiability in link monitoring. Given a set of links to monitor, our objective is to select as few probing paths as possible to cover all of them, and the selected probing paths can uniquely identify all identifiable links being monitored. We propose an algorithm based on the linear system model to find out all sets of probing paths that can uniquely identify an identifiable link. We extend the bipartite model to reflect the relation between a set of probing paths and the link that can be uniquely identified. Through the extended bipartite model, our optimization problem is transformed into the classic set cover problem, which is NP-hard. Therefore, we propose a heuristic based algorithm to greedily select the probing paths. Our method eliminates two types of redundant probing paths, i.e., those that can be replaced by others and those that cannot be used to achieving identifiability. Simulations based on real network topologies show that our approach can achieve identifiability with very low probing cost. Compared with prior work, our method is more general and has better performance.

C) NETWORK ARCHITECTURE FOR JOINT FAILURE RECOVERY AND TRAFFIC ENGINEERING

Today’s networks typically handle traffic engineering (e.g. tuning the routing-protocol parameters to optimize the flow of traffic) and failure recovery (e.g., pre-installed backup paths) independently. In this paper, we propose a unified way to balance load efficiently under a wide range of failure scenarios. Our architecture supports flexible splitting of traffic over multiple pre-computed paths, with efficient path level failure detection and automatic load balancing over the remaining paths. We propose two candidate solutions that differ in how the routers rebalance the load after a failure, leading to a trade-off between router complexity and load-balancing performance. We present and solve the optimization problems that compute the configuration state for each router. Our experiments with traffic measurements and topology data (including shared risks in the underlying transport network) from a large ISP identify a “sweet spot” that achieves near-optimal load balancing under a variety of failure scenarios, with a relatively small amount of state in the routers. We believe that our solution for joint traffic engineering and failure recovery will appeal to Internet Service Providers as well as the operators of data-center.

III. PROPOSED WORK ON REDUCING ROUTING DISTRACTION IN IP NETWORKS

A cross-layer approach is the way to minimize routing disruption caused by IP link failures. The basic idea is to consider the correlation between IP link failures in backup path selection and protect each IP link with multiple reliable backup paths. A key observation is that the backup path for an IP link is used only when the IP link fails. To develop a probabilistically correlated failure (PCF) model based on the topology mapping and the failure probability of fiber links and logical links. With the PCF model, an algorithm is proposed to select at most N reliable backup paths for each IP link and compute the rerouted traffic load on each backup path.

III. CONCLUSION

The commonly used independent and SRLG models ignore the correlation between the optical and IP layer topologies. As a result, they do not accurately reflect the correlation between logical link failures and may not select reliable backup paths. We propose a cross-layer approach for minimizing routing disruption caused by IP link failures. We develop a probabilistically correlated failure (PCF) model to quantify the impact of IP link failure on the reliability of backup paths. With this model, we propose an algorithm to minimize the routing disruption by choosing multiple reliable backup paths to protect each IP link. The proposed approach ensures that the rerouted traffic does not cause logical link overload, even when multiple logical links fail simultaneously. We evaluate our approach using real ISP networks with both optical and IP layer topologies. Experimental results show that two backup paths are adequate for protecting a logical link. Compared with existing works, the backup paths selected by our method are at least 18 percent more reliable and the routing disruption is reduced by at least 22 percent. Moreover, the proposed approach prevents logical link overload caused by the rerouted traffic.

REFERENCES

[1] Q. ZHENG, J. ZHAO, AND G. CAO, ‘‘A CROSS-LAYER APPROACH FOR IP NETWORK PROTECTION,’’ IN PROC. IEEE/IFIP DSN, 2012, PP. 1-12.
[2] Q. Zheng and G. Cao, ‘‘MINIMIZING PROBING COST AND ACHIEVING IDENTIFIABILITY IN PROBE BASED NETWORK LINK MONITORING,’’ IEEE Trans. Comput., vol. 62, no. 3, pp. 510-523, Mar. 2013.
[3] M. Suchara, D. Xu, R. Doverspike, D. Johnson, and J. Rexford, ‘‘NETWORK ARCHITECTURE FOR JOINT FAILURE RECOVERY AND TRAFFIC ENGINEERING,’’ in Proc. ACM SIGMETRICS, 2011, pp. 97-108.
[4] Q. Zheng, G. Cao, T.L. Porta, and A. Swami, ‘‘OPTIMAL RECOVERY FROM LARGE-SCALE FAILURES IN IP NETWORKS,’’ in Proc. IEEE ICDCS, 2012, pp. 295-304.
[5] M. Johnston, H.-W. Lee, and E. Modiano, ‘‘A ROBUST OPTIMIZATION APPROACH TO BACKUP NETWORK DESIGN WITH RANDOM FAILURES,’’ in Proc. IEEE INFOCOM, 2011, pp. 1512-1520.

